UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/620,176	07/20/2000	Baber Amin	1565.023US1	3893

21186 7590 01/12/2009

SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
NALVEN, ANDREW L	

ART UNIT	PAPER NUMBER
2434	

MAIL DATE	DELIVERY MODE
01/12/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte BABER AMIN and HASHEM MOHAMMAD EBRAHIMI

Appeal 2008-2009
Application 09/620,176
Technology Center 2400

Decided: January 9, 2009

Before JAY P. LUCAS, ST. JOHN COURTENAY III, and
STEPHEN C. SIU, *Administrative Patent Judges*.

SIU, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

This is a decision on appeal under 35 U.S.C. § 134(a) from the Examiner's rejection of claims 1-20. We have jurisdiction under 35 U.S.C. § 6(b). We reverse.

The Invention

The disclosed invention relates generally to interfacing application programs with network security modules (Spec. 1). Specifically, application data is received at an upper connection layer of a transport provider and passed to a security layer that encrypts the application data and passes the encrypted data to a lower connection layer. The encrypted application data is sent out over a network. The application is not required to perform security handshakes to send the encrypted application data over a network (Spec. 3).

Independent claim 1 is illustrative:

> 1. A method of providing transport-independent secure communications in a computer network, comprising the steps of:
>
> directly receiving application data, from an application, at an upper connection layer of a transport protocol stack, wherein the application data is received from the application using a connection specific application programming interface (API) desired for communication by the application and which is not associated with security;
>
> passing the application data from the upper connection layer to a security layer from within the transport protocol stack and unbeknownst to the application;
>
> encrypting the application data within the security layer;
>
> passing the encrypted application data from the security layer to a lower connection layer of the transport protocol stack; and

sending the encrypted application data from the lower connection layer out a network connection;

wherein the application is not required to perform security handshakes in order to send encrypted application data over the network, the connection layers support at least one network transport protocol, and the security layer is not specific to that transport protocol.

The References

The Examiner relies upon the following references as evidence in support of the obviousness rejection:

Samar	US 6,304,974 B1	Oct. 16, 2001 (filed Nov. 6, 1998)
Tumblin	US 6,490,679 B1	Dec. 3, 2002 (filed Jan. 18, 1999)

Shannon Appel, *[SSL-Talk List FAQ] Secure Sockets Layer Discussion List FAQ v1.1.1*, Consensus Development Corporation ("SSL"), (1998) available at http://www.consensus.com/security/ssl-talk-faq.html.

Novell, *What's Enhanced in NetWare 5*, NetWare Connection ("NetWare"), (1998) available at http://www.lansing.cc.mi.us/~jaegerm/NetWare5/WhatsEnhanced.html.

Microsoft Corporation, *SSL-Specific WSAIoctl Controls*, Microsoft Security Advisor Program ("Microsoft"), (1996).

The Rejections

1. The Examiner rejects claims 1, 2, 4, 6-9, 12, 14-18, and 20 under 35 U.S.C. § 102(e) as being anticipated by Tumblin.

2. The Examiner rejects claims 3 and 10 under 35 U.S.C. § 103(a) as being unpatentable over Tumblin and SSL.
3. The Examiner rejects claim 5 under 35 U.S.C. § 103(a) as being unpatentable over Tumblin and Samar.
4. The Examiner rejects claims 11 and 19 under 35 U.S.C. § 103(a) as being unpatentable over Tumblin and Netware.
5. The Examiner rejects claim 13 under 35 U.S.C. § 103(a) as being unpatentable over Tumblin and Microsoft.

ISSUE

The Examiner finds that Tumblin discloses "passing the application data from the upper connection layer to a security layer (Tumblin, column 8 lines 19-21 and Figure 7 Item 210, data is passed from network API to NSIM to SIM), unbeknownst to the application (Tumblin, column 8 lines 19-28, requests are intercepted by NSIM)" (Ans. 12) and that the "application is unaware that the security proceedings are commencing because the application does not recognize a security services API (Tumblin, column 3 lines 40-47)" (*id.*).

Appellants assert that "Tumblin replaces normal network communication of an application by linking in . . . the NSIM" (Reply Br. 2-3) and that "[t]he normal protocol stack communication is entirely replaced via the NSIM" (*id.* 3).

Did Appellants demonstrate that the Examiner erred in finding that Tumblin discloses receiving application data at an upper connection layer, passing the application data from the upper connection layer to a security layer unbeknownst to the application, and passing the encrypted application data from the security layer to a lower connection layer of the transport protocol stack as claimed?

FINDINGS OF FACT

The following Findings of Facts (FF) are shown by a preponderance of the evidence.

1. Tumblin discloses a client containing a "security extensible client program . . . linked to an application security interface module (ASIM)" (col. 5, ll. 14-15).
2. Tumblin discloses that a "security non-extensible client program **210** . . . is not extensible to provide additional security features" and "does not recognize a security services API **230**" (col. 3, ll. 41-45).
3. Tumblin discloses that "[i]n each security non-extensible client **210**, network access module **180** is replaced with a client network security interface module (client NSIM) **290**" that "provides the network API **190** recognized by security non-extensible application **210**" (col. 5, ll. 18-23).
4. Tumblin discloses that "[e]ach client NSIM **290** . . . is capable of receiving requests for network services from the client program **210**

. . . to which it is linked, and forwarding those requests to the network access module **180** to which it is also linked" (col. 5, ll. 42-46).

5. Tumblin discloses that "[e]ach NSIM is also capable of making requests for SKI [Security Key Infrastructure] services **270** to the SIM **310**" (col. 5, ll. 47-48).
6. Tumblin discloses "network traffic emanating from these [application] programs must pass through the NSIMs to which they are linked" (col. 8, ll. 16-17).
7. Tumblin discloses that a client requests "a new network connection" and that "the request is intercepted by the client NSIM **290** (step **710**)" (col. 8, ll. 19-24). After receiving the request, "the client NSIM **290** calls the OpenSession procedure in the SIM API" (col. 8, ll. 25-26).
8. Tumblin discloses that "if the SIM opens the new session as requested, the client NSIM **290** calls . . . [a] procedure in the SIM API, indicating the identities of the requesting host and the receiving host" (col. 8, ll. 33-36). The SIM "determines . . . whether the user and client program are authorized to make the requested connection" (col. 8, ll. 38-42).
9. Tumblin discloses that "[i]f a connection is not authorized (step **760**), the SIM returns an error message to the client NSIM **290** (step **765**),

otherwise it returns a connection policy **410** for the requested connection (step **770**)" (col. 8, ll. 42-45).

10. SSL discloses that "many SSL clients . . . check the common name of the certificate against the name of the site in the URL. If it doesn't match, the client application warns the user" (Section 5.3).
11. Samar discloses that "the user receives the signed list of certificates (step **508**)" (col. 7, l. 53), "verifies that the certificate for enterprise administrator **108** has been authenticated by the trusted certificate authority (step **510**)" (col. 7, ll. 60-62), "uses the public key of the certificate authority to verify that the certificate for enterprise administrator **108** has been validly signed by the certificate authority" (col. 7, l. 67 – col. 8, l. 3), and "uses the public key . . . to verify that the list has been signed by enterprise administrator **108**" (col. 8, ll. 3-6).
12. NetWare discloses that "NetWare 5 supports LDAP version 3" and "includes LDAP Services for NDS, which is a server-based interface between NDS and LDAP-compliant applications running under Secure Sockets Layer (SSL)" (page 1).
13. Microsoft discloses that "[a] number of SSL-specific controls have been defined for use with the **WSAIoctl** function" and that "[a]pplications can use these to enumerate an SSL . . . service provider's capabilities as well as to configure it" (page 1).

PRINCIPLES OF LAW

35 U.S.C. § 102

In rejecting claims under 35 U.S.C. § 102, "[a] single prior art reference that discloses, either expressly or inherently, each limitation of a claim invalidates that claim by anticipation." *Perricone v. Medicis Pharm. Corp.,* 432 F.3d 1368, 1375-76 (Fed. Cir. 2005) (citation omitted). "Anticipation of a patent claim requires a finding that the claim at issue 'reads on' a prior art reference." *Atlas Powder Co. v. IRECO, Inc.*, 190 F.3d 1342, 1346 (Fed Cir. 1999) ("In other words, if granting patent protection on the disputed claim would allow the patentee to exclude the public from practicing the prior art, then that claim is anticipated, regardless of whether it also covers subject matter not in the prior art.") (Internal citations omitted).

It is axiomatic that anticipation of a claim under § 102 can be found only if the prior art reference discloses every element of the claim. See *In re King*, 801 F.2d 1324, 1326 (Fed. Cir. 1986) and *Lindemann Maschinenfabrik GMBH v. American Hoist & Derrick Co.*, 730 F.2d 1452, 1458 (Fed. Cir. 1984).

35 U.S.C. § 103(a)

> Section 103 forbids issuance of a patent when "the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains."

KSR Int'l Co. v. Teleflex Inc., 127 S. Ct. 1727, 1734 (2007).

"What matters is the objective reach of the claim. If the claim extends to what is obvious, it is invalid under § 103." *KSR*, 127 S. Ct. at 1742. In *KSR*, the Supreme Court emphasized "the need for caution in granting a patent based on the combination of elements found in the prior art," and discussed circumstances in which a patent might be determined to be obvious. *Id.* at 1739 (citing *Graham v. John Deere Co.*, 383 U.S. 1, 12 (1966)). The Court reaffirmed principles based on its precedent that "[t]he combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *Id.* The operative question in this "functional approach" is thus "whether the improvement is more than the predictable use of prior art elements according to their established functions." *Id.* at 1740.

ANALYSIS

While we agree with the Examiner that Tumblin discloses a Network Security Interface Module (NSIM) linked to non-extensible client programs (see, e.g., col. 8, ll. 13-15), the Examiner has not demonstrated that Tumblin also discloses that application data is received at an upper connection layer of a transport protocol stack, passed to a security layer unbeknownst to the application, and passed to a lower connection layer of the transport protocol stack. Indeed, the Examiner has not demonstrated that Tumblin discloses a transport protocol stack at all.

The Examiner finds that Tumblin discloses that the application is "unaware that the security proceedings are commencing because the application does not recognize a security services API (Tumblin, column 3 lines 40-47)" (Ans. 12). Tumblin discloses that a non-extensible client program "is not extensible to provide additional security features" (col. 3, ll. 41-44). Thus, Tumblin discloses that because the non-extensible client program is not extensible, additional security features (i.e., security features that are in addition to those security features that the client program may already possess) are not provided. We find that this disclosure in Tumblin is not relevant to whether the application is aware of "security proceedings that are commencing" or not, nor has the Examiner provided a rationale supporting the finding that not providing additional security features in a non-extensible client (Tumblin) is equivalent to passing application data from an upper connection layer of a transport protocol stack to a security layer unbeknownst to the application.

Similarly, independent claim 7 recites a connection layer comprising an upper connection layer associated with a transport protocol stack, a lower connection layer associated with the transport protocol stack, and a security layer callable from the connection layer and unbeknownst to the application. Independent claim 16 recites a security layer receiving a request from a lower connection layer of a transport protocol stack, the application unaware of the security layer and its operations. As set forth above, we find that the Examiner has not demonstrated that Tumblin discloses a transport protocol

stack in which application data is passed unbeknownst to the application as recited.

While we agree with the Examiner that SSL discloses an application warning an SSL client if a common name of a certificate does not match a name of a URL site (FF 10), that Samar discloses a user verifying that a certificate has been authenticated and validly signed by a certificate authority (FF 11), that NetWare discloses that NetWare 5 supports LDAP (FF 12), and that Microsoft discloses SSL-specific controls that have been defined for use with a WSAIoctl function (FF13), the Examiner does not demonstrate, and we do not find, that any of Samar, SSL, NetWare, or Microsoft discloses or suggests a transport protocol stack containing an upper connection layer, security layer and lower connection layer or passing application to the security layer from the upper connection layer unbeknownst to the application.

Accordingly, we conclude that Appellants have met their burden of showing that the Examiner erred in rejecting claims 1, 2, 4, 6-9, 12, 14-18, and 20 as being anticipated by Tumblin, dependent claims 3 and 10 as being obvious over Tumblin and SSL, dependent claims 11 and 19 as being obvious over Tumblin and NetWare, dependent claim 5 as being obvious over Tumblin and Samar, and dependent claim 13 as being obvious over Tumblin and Microsoft.

CONCLUSION OF LAW

Based on the findings of facts and analysis above, we conclude that Appellants have demonstrated that the Examiner erred in finding that Tumblin discloses receiving application data at an upper connection layer, passing the application data from the upper connection layer to a security layer unbeknownst to the application, and passing the encrypted application data from the security layer to a lower connection layer of the transport protocol stack.

DECISION

We reverse the Examiner's decision rejecting claims 1, 2, 4, 6-9, 12, 14-18, and 20 under 35 U.S.C. § 102(e) and claims 3, 5, 10, 11, 13, and 19 under 35 U.S.C. § 103.

REVERSED

rwk

SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402